

Codes Associated with Orthogonal groups and Power Moments of Kloosterman Sums

Dae San Kim

Department of Mathematics, Sogang University, Seoul 121-742, Korea

Abstract In this paper, we construct three binary linear codes $C(SO^-(2, q))$, $C(O^-(2, q))$, $C(SO^-(4, q))$, respectively associated with the orthogonal groups $SO^-(2, q)$, $O^-(2, q)$, $SO^-(4, q)$, with q powers of two. Then we obtain recursive formulas for the power moments of Kloosterman and 2-dimensional Kloosterman sums in terms of the frequencies of weights in the codes. This is done via Pless power moment identity and by utilizing the explicit expressions of Gauss sums for the orthogonal groups. We emphasize that, when the recursive formulas for the power moments of Kloosterman sums are compared, the present one is computationally more effective than the previous one constructed from the special linear group $SL(2, q)$. We illustrate our results with some examples.

Index terms: Kloosterman sum, 2-dimensional Kloosterman sum, orthogonal group, Pless power moment identity, weight distribution, Gauss sum.

1 Introduction

Let ψ be a nontrivial additive character of the finite field \mathbb{F}_q with $q = p^r$ elements (p a prime), and let m be a positive integer. Then the m -dimensional Kloosterman sum $K_m(\psi; a)$ ([13]) is defined by

$$K_m(\psi; a) = \sum_{\alpha_1, \dots, \alpha_m \in \mathbb{F}_q^*} \psi(\alpha_1 + \dots + \alpha_m + a\alpha_1^{-1} \dots \alpha_m^{-1}) (a \in \mathbb{F}_q^*).$$

* Corresponding author.

Email addresses: dskim@sogang.ac.kr (Dae San Kim).

URL: <http://math.sogang.ac.kr/dskim/> (Dae San Kim).

In particular, if $m = 1$, then $K_1(\psi; a)$ is simply denoted by $K(\psi; a)$, and is

called the Kloosterman sum. The Kloosterman sum was introduced in 1926 ([11]) to give an estimate for the Fourier coefficients of modular forms.

For each nonnegative integer h , by $MK_m(\psi)^h$ we will denote the h -th moment of the m -dimensional Kloosterman sum $K_m(\psi; a)$. Namely, it is given by

$$MK_m(\psi)^h = \sum_{a \in \mathbb{F}_q^*} K_m(\psi; a)^h.$$

If $\psi = \lambda$ is the canonical additive character of \mathbb{F}_q , then $MK_m(\lambda)^h$ will be simply denoted by MK_m^h . If further $m = 1$, for brevity MK_1^h will be indicated by MK^h . The power moments of Kloosterman sums can be used, for example, to give an estimate for the Kloosterman sums and have also been studied to solve various problems in coding theory over finite fields of characteristic two.

From now on, let us assume that $q = 2^r$. Carlitz [1] evaluated MK^h , for $h \leq 4$. Recently, Moisio was able to find explicit expressions of MK^h , for $h \leq 10$ (cf. [15]) (Similar results exist also over the finite fields of characteristic three (cf. [4],[16])). This was done, via Pless power moment identity, by connecting moments of Kloosterman sums and the frequencies of weights in the binary Zetterberg code of length $q + 1$, which were known by the work of Schoof and Vlught in [19]. In [7], the binary linear codes $C(SL(n, q))$ associated with finite special linear groups $SL(n, q)$ were constructed when n, q are both powers of two. Then obtained was a recursive formula for the power moments of multi-dimensional Kloosterman sums in terms of the frequencies of weights in $C(SL(n, q))$. This was done via Pless power moment identity and by utilizing our previous result on the explicit expression of the Gauss sum for $SL(n, q)$. In particular, when $n = 2$, this gives a recursive formula for the power moments of Kloosterman sums. Also, in [8], we constructed three binary linear codes $C(SO^+(2, q))$, $C(O^+(2, q))$, $C(SO^+(4, q))$, respectively associated with $SO^+(2, q)$, $O^+(2, q)$, $SO^+(4, q)$, in order to get recursive formulas for the power moments of Kloosterman and 2-dimensional Kloosterman sums.

In this paper, we will show the following theorem giving recursive formulas for the power moments of Kloosterman and 2-dimensional Kloosterman sums. To do that, we construct three binary linear codes $C(SO^-(2, q))$, $C(O^-(2, q))$, $C(SO^-(4, q))$, respectively associated with $SO^-(2, q)$, $O^-(2, q)$, $SO^-(4, q)$, and express those power moments in terms of the frequencies of weights in each code. Then, thanks to our previous results on the explicit expressions of ‘‘Gauss sums’’ for the orthogonal group $O^-(2n, q)$ and the special orthogonal group $SO^-(2n, q)$ [10], we can express the weight of each codeword in the duals of the codes in terms of Kloosterman or 2-dimensional Kloosterman sums. Then our formulas will follow immediately from the Pless power moment identity.

The recursive formula for power moments of Kloosterman sums in this paper

(cf. (1), (2)) is computationally more effective than that in [7](cf. [7], (3)). This is because it is easier to compute the weight distribution of $C(SO^-(2, q))$ than that of $C(SL(2, q))$. Theorem 1 in the following is the main result of this paper.

Theorem 1 : *Let $q = 2^r$. Then we have the following.*

(a) *For $h = 1, 2, \dots$,*

$$MK^h = - \sum_{l=0}^{h-1} \binom{h}{l} (q+1)^{h-l} MK^l + q \sum_{j=0}^{\min\{N_1, h\}} (-1)^j C_{1,j} \sum_{t=j}^h t! S(h, t) 2^{h-t} \binom{N_1 - j}{N_1 - t}, \quad (1)$$

where $N_1 = |SO^-(2, q)| = q + 1$, and $\{C_{1,j}\}_{j=0}^{N_1}$ is the weight distribution of $C(SO^-(2, q))$ given by

$$C_{1,j} = \sum \binom{1}{\nu_0} \prod_{tr(\beta^{-1})=1} \binom{2}{\nu_\beta} (j = 0, \dots, N_1). \quad (2)$$

Here the sum is over all the sets of nonnegative integers $\{\nu_0\} \cup \{\nu_\beta\}_{tr(\beta^{-1})=1}$ satisfying $\nu_0 + \sum_{tr(\beta^{-1})=1} \nu_\beta = j$ and $\sum_{tr(\beta^{-1})=1} \nu_\beta \beta = 0$. In addition, $S(h, t)$ is the Stirling number of the second kind defined by

$$S(h, t) = \frac{1}{t!} \sum_{j=0}^t (-1)^{t-j} \binom{t}{j} j^h. \quad (3)$$

(b) *For $h = 1, 2, \dots$,*

$$MK^h = - \sum_{l=0}^{h-1} \binom{h}{l} (q+1)^{h-l} MK^l + q \sum_{j=0}^{\min\{N_2, h\}} (-1)^j C_{2,j} \sum_{t=j}^h t! S(h, t) 2^{h-t} \binom{N_2 - j}{N_2 - t}, \quad (4)$$

where $N_2 = |O^-(2, q)| = 2(q + 1)$, and $\{C_{2,j}\}_{j=0}^{N_2}$ is the weight distribution of $C(O^-(2, q))$ given by

$$C_{2,j} = \sum \binom{q+2}{\nu_0} \prod_{tr(\beta^{-1})=1} \binom{2}{\nu_\beta} (j = 0, \dots, N_2). \quad (5)$$

Here the sum is over all the sets of nonnegative integers $\{\nu_0\} \cup \{\nu_\beta\}_{tr(\beta^{-1})=1}$

satisfying $\nu_0 + \sum_{\text{tr}(\beta^{-1})=1} \nu_\beta = j$ and $\sum_{\text{tr}(\beta^{-1})=1} \nu_\beta \beta = 0$.

(c) For $r \geq 2$, and $h = 1, 2, \dots$,

$$MK_2^h = - \sum_{l=0}^{h-1} \binom{h}{l} (q^4 + q^3 - 1)^{h-l} MK_2^l + q^{1-2h} \sum_{j=0}^{\min\{N_3, h\}} (-1)^j C_{3,j} \sum_{t=j}^h t! S(h, t) 2^{h-t} \binom{N_3 - j}{N_3 - t}, \quad (6)$$

$$MK^{2h} = - \sum_{l=0}^{h-1} \binom{h}{l} (q^4 + q^3 - q - 1)^{h-l} MK^{2l} + q^{1-2h} \sum_{j=0}^{\min\{N_3, h\}} (-1)^j C_{3,j} \sum_{t=j}^h t! S(h, t) 2^{h-t} \binom{N_3 - j}{N_3 - t}, \quad (7)$$

where $N_3 = |SO^-(4, q)| = q^2(q^4 - 1)$, and $\{C_{3,j}\}_{j=0}^{N_3}$ is the weight distribution of $C(SO^-(4, q))$ given by

$$C_{3,j} = \sum \binom{m_0}{\nu_0} \prod_{\substack{|t| < 2\sqrt{q} \\ t \equiv -1(4)}} \prod_{K(\lambda; \beta^{-1})=t} \binom{m_t}{\nu_\beta} (j = 0, \dots, N_3). \quad (8)$$

Here the sum is over all the sets of nonnegative integers $\{\nu_\beta\}_{\beta \in \mathbb{F}_q}$ satisfying $\sum_{\beta \in \mathbb{F}_q} \nu_\beta = j$ and $\sum_{\beta \in \mathbb{F}_q} \nu_\beta \beta = 0$,

$$m_0 = q^4,$$

and

$$m_t = q^2(q^3 + q^2 - t),$$

for all integers t satisfying $|t| < 2\sqrt{q}$, and $t \equiv -1 \pmod{4}$.

2 $O^-(2n, q)$

For more details about the results of this section, one is referred to the paper [10]. Also, we recommend [20] as a general reference for matrix groups over

finite fields. Throughout this paper, the following notations will be used:

$$q = 2^r \ (r \in \mathbb{Z}_{>0}),$$

\mathbb{F}_q = the finite field with q elements,

$Tr A$ = the trace of A for a square matrix A ,

${}^t B$ = the transpose of B for any matrix B .

Let θ^- be the nondegenerate quadratic form on the vector space $\mathbb{F}_q^{2n \times 1}$ of all $2n \times 1$ column vectors over \mathbb{F}_q , given by

$$\theta^-\left(\sum_{i=1}^{2n} x_i e^i\right) = \sum_{i=1}^{n-1} x_i x_{n-1+i} + x_{2n-1}^2 + x_{2n-1} x_{2n} + a x_{2n}^2, \quad (9)$$

where $\{e^1 = {}^t [10 \dots 0], e^2 = {}^t [010 \dots 0], \dots, e^{2n} = {}^t [0 \dots 01]\}$ is the standard basis of $\mathbb{F}_q^{2n \times 1}$, and a is a fixed element in \mathbb{F}_q such that $z^2 + z + a$ is irreducible over \mathbb{F}_q , or equivalently $a \in \mathbb{F}_q \setminus \Theta(\mathbb{F}_q)$, where $\Theta(\mathbb{F}_q) = \{\alpha^2 + \alpha | \alpha \in \mathbb{F}_q\}$ is a subgroup of index 2 in the additive group \mathbb{F}_q^+ of \mathbb{F}_q .

Let δ_a (with a in the above paragraph), η denote respectively the 2×2 matrices over \mathbb{F}_q , given by:

$$\delta_a = \begin{bmatrix} 1 & 1 \\ 0 & a \end{bmatrix} z, \quad \eta = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}. \quad (10)$$

Then the group $O^-(2n, q)$ of all isometries of $(\mathbb{F}_q^{2n \times 1}, \theta^-)$ consists of all matrices

$$\begin{bmatrix} A & B & e \\ C & D & f \\ g & h & i \end{bmatrix} \quad (A, B, C, D(n-1) \times (n-1), \ e, f(n-1) \times 2, \ g, \ h \ 2 \times (n-1)) \quad (11)$$

in $GL(2n, q)$ satisfying the relations:

$${}^t A C + {}^t g \delta_a g \text{ is alternating,}$$

$$\begin{aligned}
& {}^tBD + {}^th\delta_a h \text{ is alternating,} \\
& {}^tef + {}^ti\delta_a i + \delta_a \text{ is alternating,} \\
& {}^tAD + {}^tCB + {}^tg\eta h = 1_{n-1}, \\
& {}^tAf + {}^tCe + {}^tg\eta i = 0, \\
& {}^tBf + {}^tDe + {}^th\eta i = 0.
\end{aligned} \tag{12}$$

Here an $n \times n$ matrix (a_{ij}) is called alternating if

$$\begin{cases} a_{ii} = 0, & \text{for } 1 \leq i \leq n, \\ a_{ij} = -a_{ji} = a_{ji}, & \text{for } 1 \leq i < j \leq n. \end{cases}$$

$P^- = P^-(2n, q)$ is the maximal parabolic subgroup of $O^-(2n, q)$ defined by:

$$P^-(2n, q) = \left\{ \begin{bmatrix} A & 0 & 0 \\ 0 & {}^tA^{-1} & 0 \\ 0 & 0 & i \end{bmatrix} \begin{bmatrix} 1_{n-1} & B & {}^th{}^ti\eta i \\ 0 & 1_{n-1} & 0 \\ 0 & h & 1_2 \end{bmatrix} \middle| \begin{array}{l} A \in GL(n-1, q), \ i \in O^-(2, q), \\ {}^tB + {}^th\delta_a h \text{ is alternating} \end{array} \right\},$$

where $O^-(2, q)$ is the group of all isometries of $(\mathbb{F}_q^{2 \times 1}, \theta^-)$, with

$$\theta^-(x_1 e^1 + x_2 e^2) = x_1^2 + x_1 x_2 + a x_2^2. \quad (\text{cf. (9)})$$

One can show that

$$O^-(2, q) = SO^-(2, q) \coprod \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix} SO^-(2, q), \tag{13}$$

$$\begin{aligned}
SO^-(2, q) &= \left\{ \begin{bmatrix} d_1 & ad_2 \\ d_2 & d_1 + d_2 \end{bmatrix} \middle| d_1^2 + d_1 d_2 + ad_2^2 = 1 \right\} \\
&= \left\{ \begin{bmatrix} d_1 & ad_2 \\ d_2 & d_1 + d_2 \end{bmatrix} \middle| d_1 + d_2 b \in \mathbb{F}_q(b), \text{ with } N_{\mathbb{F}_q(b)/\mathbb{F}_q}(d_1 + d_2 b) = 1 \right\},
\end{aligned}$$

where $b \in \overline{\mathbb{F}_q}$ is a root of the irreducible polynomial $z^2 + z + a$ over \mathbb{F}_q . $SO^-(2, q)$ is a subgroup of index 2 in $O^-(2, q)$ and

$$|SO^-(2, q)| = q + 1, \quad |O^-(2, q)| = 2(q + 1).$$

$SO^-(2, q)$ here is defined as the kernel of a certain epimorphism $\delta^- : O^-(2n, q) \rightarrow \mathbb{F}_2^+$, to be defined below.

The Bruhat decomposition of $O^-(2n, q)$ with respect to $P^- = P^-(2n, q)$ is

$$O^-(2n, q) = \prod_{r=0}^{n-1} P^- \sigma_r^- P^-, \quad (14)$$

where

$$\sigma_r^- = \begin{bmatrix} 0 & 0 & 1_r & 0 & 0 \\ 0 & 1_{n-1-r} & 0 & 0 & 0 \\ 1_r & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1_{n-1-r} & 0 \\ 0 & 0 & 0 & 0 & 1_2 \end{bmatrix} \in O^-(2n, q).$$

For each r , with $0 \leq r \leq n-1$, put

$$A_r^- = \{w \in P^-(2n, q) \mid \sigma_r^- w (\sigma_r^-)^{-1} \in P^-(2n, q)\}.$$

As a disjoint union of right cosets of $P^- = P^-(2n, q)$, the Bruhat decomposition in (14) can be written as

$$O^-(2n, q) = \prod_{r=0}^{n-1} P^- \sigma_r^- (A_r^- \setminus P^-). \quad (15)$$

The order of the general linear group $GL(n, q)$ is given by

$$g_n = \prod_{j=0}^{n-1} (q^n - q^j) = q^{\binom{n}{2}} \prod_{j=1}^n (q^j - 1).$$

For integers n, r with $0 \leq r \leq n$, the q -binomial coefficients are defined as:

$$\begin{bmatrix} n \\ r \end{bmatrix}_q = \prod_{j=0}^{r-1} (q^{n-j} - 1) / (q^{r-j} - 1). \quad (16)$$

Then, for integers n, r with $0 \leq r \leq n$, we have

$$\frac{g_n}{g_{n-r} g_r} = q^{r(n-r)} \begin{bmatrix} n \\ r \end{bmatrix}_q. \quad (17)$$

In [10], it is shown

$$|A_r^-| = 2(q+1)g_r g_{n-1-r} q^{(n-1)(n+2)/2} q^{r(2n-3r-5)/2}, \quad (18)$$

$$|P^-(2n, q)| = 2(q+1)g_{n-1}q^{(n-1)(n+2)/2}. \quad (19)$$

So, from (17)-(19), we get:

$$|A_r^- \setminus P^-(2n, q)| = \begin{bmatrix} n-1 \\ r \end{bmatrix}_q q^{r(r+3)/2}, \quad (20)$$

and

$$|P^-(2n, q)|^2 |A_r^-|^{-1} = 2(q+1)q^{n^2-n} \prod_{j=1}^{n-1} (q^j - 1) \begin{bmatrix} n-1 \\ r \end{bmatrix}_q q^{\binom{r}{2}} q^{2r}. \quad (21)$$

As one consequence of these computations, from (15) and (21), we are able to get the order of $O^-(2n, q)$.

$$\begin{aligned} |O^-(2n, q)| &= \sum_{r=0}^{n-1} |P^-(2n, q)|^2 |A_r^-|^{-1} \\ &= 2q^{n^2-n} (q^n + 1) \prod_{j=1}^{n-1} (q^{2j} - 1), \end{aligned} \quad (22)$$

where one needs to apply the following q -binomial theorem with $x = -q^2$:

$$\sum_{r=0}^n \begin{bmatrix} n \\ r \end{bmatrix}_q (-1)^r q^{\binom{r}{2}} x^r = (x; q)_n,$$

with $(x; q)_n = (1-x)(1-qx) \cdots (1-q^{n-1}x)$ (x an indeterminate, $n \in \mathbb{Z}_{>0}$).

Related to the Clifford algebra $C(\mathbb{F}_q^{2n \times 1}, \theta^-)$ of the quadratic space $(\mathbb{F}_q^{2n \times 1}, \theta^-)$, there is an epimorphism of groups $\delta^- : O^-(2n, q) \rightarrow \mathbb{F}_2^+$, which is given by

$$\delta^-(w) = Tr({}^t h \delta_a g) + Tr\left(e \begin{bmatrix} 0 & 0 \\ 1 & 0 \end{bmatrix} {}^t f\right) + Tr(B {}^t C) + {}^t i^2 \delta_a i^1,$$

where δ_a is as in (10), $i = [i^1 i^2]$ with i^1, i^2 denoting the first and second columns of i , and

$$w = \begin{bmatrix} A & B & e \\ C & D & f \\ g & h & i \end{bmatrix} \in O^-(2n, q) \quad (\text{cf. (11), (12)}).$$

In order to describe $SO^-(2n, q)$, we introduce a subgroup $Q^-(2n, q)$ of index 2 in $P^-(2n, q)$, defined by:

$$\begin{aligned} Q^- &= Q^-(2n, q) \\ &= \left\{ \begin{bmatrix} A & 0 & 0 \\ 0 & {}^tA^{-1} & 0 \\ 0 & 0 & i \end{bmatrix} \begin{bmatrix} 1_{n-1} & B & {}^th^ti\eta i \\ 0 & 1_{n-1} & 0 \\ 0 & h & 1_2 \end{bmatrix} \mid \begin{array}{l} A \in GL(n-1, q), i \in SO^-(2, q), \\ {}^tB + {}^th\delta_a h \text{ is alternating} \end{array} \right\}. \end{aligned}$$

Also, for each r , with $0 \leq r \leq n-1$, we define

$$B_r^- = \{w \in Q^-(2n, q) \mid \sigma_r^- w (\sigma_r^-)^{-1} \in P^-(2n, q)\}.$$

which is a subgroup of index 2 in A_r^- .

The decompositions in (14) and (15) can be modified so as to give:

$$O^-(2n, q) = \prod_{r=0}^{n-1} P^- \sigma_r^- Q^-,$$

$$O^-(2n, q) = \prod_{r=0}^{n-1} P^- \sigma_r^- (B_r^- \setminus Q^-), \quad (23)$$

and

$$|B_r^- \setminus Q^-| = |A_r^- \setminus P^-| \quad (\text{cf. (20)}).$$

$SO^-(2n, q) := \text{Ker} \delta^-$ is given by

$$\begin{aligned} SO^-(2n, q) &= \left(\prod_{0 \leq r \leq n-1, r \text{ even}} Q^- \sigma_r^- (B_r^- \setminus Q^-) \right) \\ &\quad \prod_{0 \leq r \leq n-1, r \text{ odd}} (\rho Q^- \sigma_r^- (B_r^- \setminus Q^-)), \end{aligned} \quad (24)$$

with

$$\rho = \begin{bmatrix} 1_{n-1} & 0 & 0 & 0 \\ 0 & 1_{n-1} & 0 & 0 \\ 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 1 \end{bmatrix} \in P^-(2n, q),$$

and

$$|SO^-(2n, q)| = q^{n^2-n}(q^n + 1) \prod_{j=1}^{n-1} (q^{2j} - 1) \text{ (cf. (20)).}$$

3 Gauss sums for $O^-(2n, q)$

The following notations will be used throughout this paper.

$$\begin{aligned} \text{tr}(x) &= x + x^2 + \cdots + x^{2^{r-1}} \text{ the trace function } \mathbb{F}_q \rightarrow \mathbb{F}_2, \\ \lambda(x) &= (-1)^{\text{tr}(x)} \text{ the canonical additive character of } \mathbb{F}_q. \end{aligned}$$

Then any nontrivial additive character ψ of \mathbb{F}_q is given by $\psi(x) = \lambda(ax)$, for a unique $a \in \mathbb{F}_q^*$.

For any nontrivial additive character ψ of \mathbb{F}_q and $a \in \mathbb{F}_q^*$, the Kloosterman sum $K_{GL(t,q)}(\psi; a)$ for $GL(t, q)$ is defined as

$$K_{GL(t,q)}(\psi; a) = \sum_{w \in GL(t,q)} \psi(\text{Tr} w + a \text{Tr} w^{-1}). \quad (25)$$

Observe that, for $t = 1$, $K_{GL(1,q)}(\psi; a)$ denotes the Kloosterman sum $K(\psi; a)$.

For the Kloosterman sum $K(\psi; a)$, we have the Weil bound (cf. [13])

$$|K(\psi; a)| \leq 2\sqrt{q}. \quad (26)$$

In [6], it is shown that $K_{GL(t,q)}(\psi; a)$ satisfies the following recursive relation: for integers $t \geq 2$, $a \in \mathbb{F}_q^*$,

$$\begin{aligned} K_{GL(t,q)}(\psi; a) &= q^{t-1} K_{GL(t-1,q)}(\psi; a) K(\psi; a) \\ &\quad + q^{2t-2} (q^{t-1} - 1) K_{GL(t-2,q)}(\psi; a), \end{aligned} \quad (27)$$

where we understand that $K_{GL(0,q)}(\psi; a) = 1$. From (27), in [6] an explicit expression of the Kloosterman sum for $GL(t, q)$ was derived.

Theorem 2 ([6]): For integers $t \geq 1$, and $a \in \mathbb{F}_q^*$, the Kloosterman sum $K_{GL(t,q)}(\psi; a)$ is given by

$$K_{GL(t,q)}(\psi; a) = q^{(t-2)(t+1)/2} \sum_{l=1}^{[(t+2)/2]} q^l K(\psi; a)^{t+2-2l} \sum \prod_{\nu=1}^{l-1} (q^{j_\nu-2\nu} - 1),$$

where $K(\psi; a)$ is the Kloosterman sum and the inner sum is over all integers j_1, \dots, j_{l-1} satisfying $2l-1 \leq j_{l-1} \leq j_{l-2} \leq \dots \leq j_1 \leq t+1$. Here we agree that the inner sum is 1 for $l=1$.

Proposition 3 : Let ψ be a nontrivial additive character of \mathbb{F}_q . Then

$$(a) \quad \sum_{i \in SO^-(2,q)} \psi(Tr i) = -K(\psi; 1), \quad (28)$$

$$(b) \quad \sum_{i \in O^-(2,q)} \psi(Tr i) = -K(\psi; 1) + q + 1. \quad (29)$$

PROOF. From (13),

$$\sum_{i \in O^-(2,q)} \psi(Tr i) = \sum_{i \in SO^-(2,q)} \psi(Tr i) + \sum_{i \in SO^-(2,q)} \psi(Tr \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix} i),$$

the first and second sums of which are respectively equal to $-K(\psi; 1)$ and $q+1$ ([9], Prop. 3.1). \square

Proposition 4 ([10], Prop. 4.4): Let ψ be a nontrivial additive character of \mathbb{F}_q . For each positive integer r , let Ω_r be the set of all $r \times r$ nonsingular symmetric matrices over \mathbb{F}_q . Then the $b_r(\psi)$ defined below is independent of ψ , and is equal to:

$$b_r = b_r(\psi) = \sum_{B \in \Omega_r} \sum_{h \in \mathbb{F}_q^{r \times 2}} \psi(Tr \delta_a^t h B h) \quad (30)$$

$$= \begin{cases} q^{r(r+6)/4} \prod_{j=1}^{r/2} (q^{2j-1} - 1), & \text{for } r \text{ even,} \\ -q^{(r^2+4r-1)/4} \prod_{j=1}^{(r+1)/2} (q^{2j-1} - 1), & \text{for } r \text{ odd.} \end{cases}$$

In Section 5 of [10], it is shown that the Gauss sums for $O^-(2n, q)$ and $SO^-(2n, q)$ are respectively given by (cf. (16), (23)-(25), (30)) :

$$\begin{aligned}
& \sum_{w \in O^-(2n, q)} \psi(Trw) \\
&= \sum_{r=0}^{n-1} |B_r^- \setminus Q^-| \sum_{w \in P^-} \psi(Trw\sigma_r^-) \\
&= q^{(n-1)(n+2)/2} (-K(\psi; 1) + q + 1) \sum_{r=0}^{n-1} \begin{bmatrix} n-1 \\ r \end{bmatrix}_q q^{r(2n-r-3)/2} b_r K_{GL(n-1-r, q)}(\psi; 1), \\
& \sum_{w \in SO^-(2n, q)} \psi(Trw) \\
&= \sum_{0 \leq r \leq n-1, r \text{ even}} |B_r^- \setminus Q^-| \sum_{w \in Q^-} \psi(Trw\sigma_r^-) \\
&+ \sum_{0 \leq r \leq n-1, r \text{ odd}} |B_r^- \setminus Q^-| \sum_{w \in Q^-} \psi(Tr\rho w\sigma_r^-) \\
&= q^{(n-1)(n+2)/2} \left\{ -K(\psi; 1) \sum_{0 \leq r \leq n-1, r \text{ even}} \begin{bmatrix} n-1 \\ r \end{bmatrix}_q q^{r(2n-r-3)/2} b_r K_{GL(n-1-r, q)}(\psi; 1) \right. \\
&\quad \left. + (q + 1) \sum_{0 \leq r \leq n-1, r \text{ odd}} \begin{bmatrix} n-1 \\ r \end{bmatrix}_q q^{r(2n-r-3)/2} b_r K_{GL(n-1-r, q)}(\psi; 1) \right\}.
\end{aligned} \tag{31}$$

Here ψ is any nontrivial additive character of \mathbb{F}_q . For our purposes, we only need the following three expressions of the Gauss sums for $SO^-(2, q)$, $O^-(2, q)$, and $SO^-(4, q)$. So we state them separately as a theorem (cf. (28), (29), (31)). Also, for the ease of notations, we introduce

$$G_1(q) = SO^-(2, q), G_2(q) = O^-(2, q), G_3(q) = SO^-(4, q).$$

Theorem 5 : Let ψ be any nontrivial additive character of \mathbb{F}_q . Then we have

$$\begin{aligned}
\sum_{w \in G_1(q)} \psi(Trw) &= -K(\psi; 1), \\
\sum_{w \in G_2(q)} \psi(Trw) &= -K(\psi; 1) + q + 1, \\
\sum_{w \in G_3(q)} \psi(Trw) &= -q^2(K(\psi; 1)^2 + q^3 - q).
\end{aligned}$$

Proposition 6 ([8]): For $n = 2^s (s \in \mathbb{Z}_{\geq 0})$, and ψ a nontrivial additive character of \mathbb{F}_q ,

$$K(\psi; a^n) = K(\psi; a).$$

For the next corollary, we need a result of Carlitz.

Theorem 7 ([2]): For the canonical additive character λ of \mathbb{F}_q , and $a \in \mathbb{F}_q^*$,

$$K_2(\psi; a) = K(\psi; a)^2 - q. \quad (32)$$

The next corollary follows from Theorems 5 and 7, Proposition 6, and by simple change of variables.

Corollary 8 : Let λ be the canonical additive character of \mathbb{F}_q , and let $a \in \mathbb{F}_q^*$. Then we have

$$\sum_{w \in G_1(q)} \lambda(a \text{Tr} w) = -K(\lambda; a), \quad (33)$$

$$\sum_{w \in G_2(q)} \lambda(a \text{Tr} w) = -K(\lambda; a) + q + 1, \quad (34)$$

$$\sum_{w \in G_3(q)} \lambda(a \text{Tr} w) = -q^2(K(\lambda; a)^2 + q^3 - q) \quad (35)$$

$$= -q^2(K_2(\lambda; a) + q^3). \quad (36)$$

Proposition 9 ([8]): Let λ be the canonical additive character of \mathbb{F}_q , $m \in \mathbb{Z}_{>0}$, $\beta \in \mathbb{F}_q$. Then

$$\begin{aligned} & \sum_{a \in \mathbb{F}_q^*} \lambda(-a\beta) K_m(\lambda; a) \\ &= \begin{cases} q K_{m-1}(\lambda; \beta^{-1}) + (-1)^{m+1}, & \text{if } \beta \neq 0, \\ (-1)^{m+1}, & \text{if } \beta = 0, \end{cases} \end{aligned} \quad (37)$$

with the convention $K_0(\lambda; \beta^{-1}) = \lambda(\beta^{-1})$.

Let $G(q)$ be one of finite classical groups over \mathbb{F}_q . Then we put, for each $\beta \in \mathbb{F}_q$,

$$N_{G(q)}(\beta) = |\{w \in G(q) \mid \text{Tr}(w) = \beta\}|.$$

Then it is easy to see that

$$q N_{G(q)}(\beta) = |G(q)| + \sum_{a \in \mathbb{F}_q^*} \lambda(-a\beta) \sum_{w \in G(q)} \lambda(a \text{Tr} w). \quad (38)$$

For brevity, we write

$$n_1(\beta) = N_{G_1(q)}(\beta), \quad n_2(\beta) = N_{G_2(q)}(\beta), \quad n_3(\beta) = N_{G_3(q)}(\beta). \quad (39)$$

Using (33), (34), (36)–(38), one derives the following.

Proposition 10 : With $n_1(\beta), n_2(\beta), n_3(\beta)$ as in (39), we have

$$n_1(\beta) = \begin{cases} 1, & \text{if } \beta = 0, \\ 2, & \text{if } \beta \neq 0 \text{ with } \text{tr}(\beta^{-1}) = 1, \\ 0, & \text{if } \beta \neq 0 \text{ with } \text{tr}(\beta^{-1}) = 0, \end{cases} \quad (40)$$

$$n_2(\beta) = \begin{cases} q+2, & \text{if } \beta = 0, \\ 2, & \text{if } \beta \neq 0 \text{ with } \text{tr}(\beta^{-1}) = 1, \\ 0, & \text{if } \beta \neq 0 \text{ with } \text{tr}(\beta^{-1}) = 0, \end{cases} \quad (41)$$

$$n_3(\beta) = \begin{cases} q^4, & \text{if } \beta = 0, \\ q^2\{q^3 + q^2 - K(\lambda; \beta^{-1})\}, & \text{if } \beta \neq 0. \end{cases} \quad (42)$$

4 Construction of codes

Let

$$N_1 = |G_1(q)| = q+1, \quad N_2 = |G_2(q)| = 2(q+1), \quad N_3 = |G_3(q)| = q^2(q^4-1). \quad (43)$$

Here we will construct three binary linear codes $C(G_1(q))$ of length N_1 , $C(G_2(q))$ of length N_2 , and $C(G_3(q))$ of length N_3 , respectively associated with the orthogonal groups $G_1(q)$, $G_2(q)$, and $G_3(q)$.

By abuse of notations, for $i = 1, 2, 3$, let g_1, g_2, \dots, g_{N_i} be a fixed ordering of the elements in the group $G_i(q)$.

Also, for $i = 1, 2, 3$, we put

$$v_i = (\text{Tr}g_1, \text{Tr}g_2, \dots, \text{Tr}g_{N_i}) \in \mathbb{F}_q^{N_i}.$$

Then, for $i = 1, 2, 3$, the binary linear code $C(G_i(q))$ is defined as

$$C(G_i(q)) = \{u \in \mathbb{F}_2^{N_i} \mid u \cdot v_i = 0\}, \quad (44)$$

where the dot denotes the usual inner product in $\mathbb{F}_q^{N_i}$.

The following Delsarte's theorem is well-known.

Theorem 11 ([14]): Let B be a linear code over \mathbb{F}_q . Then

$$(B|_{\mathbb{F}_2})^\perp = \text{tr}(B^\perp).$$

In view of this theorem, the dual $C(G_i(q))^\perp (i = 1, 2, 3)$ is given by

$$C(G_i(q))^\perp = \{c(a) = (tr(aTrg_1), \dots, tr(aTrg_{N_i})) | a \in \mathbb{F}_q\}. \quad (45)$$

Let $\mathbb{F}_2^+, \mathbb{F}_q^+$ denote the additive groups of the fields $\mathbb{F}_2, \mathbb{F}_q$, respectively. Then, with $\Theta(x) = x^2 + x$ denoting the Artin-Schreier operator in characteristic two, we have the following exact sequence of groups:

$$0 \rightarrow \mathbb{F}_2^+ \rightarrow \mathbb{F}_q^+ \rightarrow \Theta(\mathbb{F}_q) \rightarrow 0.$$

Here the first map is the inclusion and the second one is given by $x \mapsto \Theta(x) = x^2 + x$. So

$$\Theta(\mathbb{F}_q) = \{\alpha^2 + \alpha \mid \alpha \in \mathbb{F}_q\}, \text{ and } [\mathbb{F}_q^+ : \Theta(\mathbb{F}_q)] = 2. \quad (46)$$

Theorem 12 ([8]): Let λ be the canonical additive character of \mathbb{F}_q , and let $\beta \in \mathbb{F}_q^*$. Then

$$\begin{aligned} (a) \quad \sum_{\alpha \in \mathbb{F}_q - \{0,1\}} \lambda\left(\frac{\beta}{\alpha^2 + \alpha}\right) &= K(\lambda; \beta) - 1, \\ (b) \quad \sum_{\alpha \in \mathbb{F}_q} \lambda\left(\frac{\beta}{\alpha^2 + \alpha + b}\right) &= -K(\lambda; \beta) - 1, \end{aligned} \quad (47)$$

if $x^2 + x + b (b \in \mathbb{F}_q)$ is irreducible over \mathbb{F}_q , or equivalently if $b \in \mathbb{F}_q \setminus \Theta(\mathbb{F}_q)$ (cf. (46)).

Theorem 13 : For any $q = 2^r$, the map $\mathbb{F}_q \rightarrow C(G_i(q))^\perp (a \mapsto c(a))$, for $i = 1, 2, 3$, is an \mathbb{F}_2 -linear isomorphism.

PROOF. Since $G_2(q)$ case can be shown in exactly the same manner as $G_1(q)$ case, we will treat $G_1(q)$ and $G_3(q)$ cases. Let $i = 1$. The map is clearly \mathbb{F}_2 -linear and surjective. Let a be in the kernel of the map. Then $tr(aTrg) = 0$, for all $g \in G_1(q)$. Since $n_1(\beta) = |\{g \in G_1(q) | Tr(g) = \beta\}| = 2$, for all $\beta \in \mathbb{F}_q^*$ with $tr(\beta^{-1}) = 1$ (cf. (40)), $tr(a\beta) = 0$, for all $\beta \in \mathbb{F}_q^*$ with $tr(\beta^{-1}) = 1$. Let $b \in \mathbb{F}_q \setminus \Theta(\mathbb{F}_q)$. Then $tr(\gamma) = 1 \Leftrightarrow \gamma = \alpha^2 + \alpha + b$, for some $\alpha \in \mathbb{F}_q$. As $z^2 + z + b$ is irreducible over \mathbb{F}_q , $\alpha^2 + \alpha + b \neq 0$, for all $\alpha \in \mathbb{F}_q$, and hence $tr(\frac{a}{\alpha^2 + \alpha + b}) = 0$, for all $\alpha \in \mathbb{F}_q$. So $\sum_{\alpha \in \mathbb{F}_q} \lambda(\frac{a}{\alpha^2 + \alpha + b}) = q$. Assume now that $a \neq 0$. Then, from (26), (47),

$$q = -K(\lambda; a) - 1 \leq 2\sqrt{q} - 1.$$

But this is impossible, since $x > 2\sqrt{x} - 1$, for $x \geq 2$.

Now, let $i = 3$. Again, the map is \mathbb{F}_2 -linear and surjective. From (42) and using the Weil bound in (26), we see that $n_3(\beta) = |\{g \in G_3(q) | Tr(g) = \beta\}| > 0$, for

all $\beta \in \mathbb{F}_q$. Let a be in the kernel. Then $\text{tr}(a\text{Tr}g) = 0$, for all $g \in G_3(q)$, and hence $\text{tr}(a\beta) = 0$, for all $\beta \in \mathbb{F}_q$. This implies that $a = 0$, since otherwise $\text{tr} : \mathbb{F}_q \rightarrow \mathbb{F}_2$ would be the trivial map. \square

5 Power moments of Kloosterman sums

In this section, we will be able to find, via Pless power moment identity, a recursive formula for the power moments of Kloosterman sums in terms of the frequencies of weights in $C(G_i(q))$, for each $i = 1, 2, 3$.

Theorem 14 (*Pless power moment identity*): Let B be an q -ary $[n, k]$ code, and let B_i (resp. B_i^\perp) denote the number of codewords of weight i in B (resp. in B^\perp). Then, for $h = 0, 1, 2, \dots$,

$$\sum_{j=0}^n j^h B_j = \sum_{j=0}^{\min\{n, h\}} (-1)^j B_j^\perp \sum_{t=j}^h t! S(h, t) q^{k-t} (q-1)^{t-j} \binom{n-j}{n-t}, \quad (48)$$

where $S(h, t)$ is the Stirling number of the second kind defined in (3).

Recall that, for $i = 1, 2, 3$, every codeword in $C(G_i(q))^\perp$ can be written as $c(a)$, for a unique $a \in \mathbb{F}_q$ (cf. Theorem 13, (45)).

Lemma 15 : Let $c(a) = (\text{tr}(a\text{Tr}g_1), \dots, \text{tr}(a\text{Tr}g_{N_i})) \in C(G_i(q))^\perp$, for $a \in \mathbb{F}_q^*$, and $i = 1, 2, 3$. Then the Hamming weight $w(c(a))$ can be expressed as follows:

$$(a) \quad \text{For } i = 1, 2, \quad w(c(a)) = \frac{1}{2}(q+1+K(\lambda; a)), \quad (49)$$

$$(b) \quad \text{For } i = 3, \quad w(c(a)) = \frac{1}{2}q^2(q^4 + q^3 - q - 1 + K(\lambda; a)^2) \\ = \frac{1}{2}q^2(q^4 + q^3 - 1 + K_2(\lambda; a)). \quad (50)$$

PROOF. For $i = 1, 2, 3$,

$$\begin{aligned} w(c(a)) &= \frac{1}{2} \sum_{j=1}^{N_i} (1 - (-1)^{\text{tr}(a \text{Tr} g_j)}) \\ &= \frac{1}{2} (N_i - \sum_{w \in G_i(q)} \lambda(a \text{Tr} w)). \end{aligned}$$

Our results now follow from (43) and (33)-(36). \square

Fix i ($i = 1, 2, 3$), and let $u = (u_1, \dots, u_{N_i}) \in \mathbb{F}_2^{N_i}$, with ν_β 1's in the coordinate places where $\text{Tr}(g_j) = \beta$, for each $\beta \in \mathbb{F}_q$. Then we see from the definition of the code $C(G_i(q))$ (cf. (45)) that u is a codeword with weight j if and only if $\sum_{\beta \in \mathbb{F}_q} \nu_\beta = j$ and $\sum_{\beta \in \mathbb{F}_q} \nu_\beta \beta = 0$ (an identity in \mathbb{F}_q). As there are $\prod_{\beta \in \mathbb{F}_q} \binom{n_i(\beta)}{\nu_\beta}$ many such codewords with weight j , we obtain the following result.

Proposition 16 : Let $\{C_{i,j}\}_{j=0}^{N_i}$ be the weight distribution of $C(G_i(q))$, for each $i = 1, 2, 3$, where $C_{i,j}$ denotes the frequency of the codewords with weight j in $C(G_i(q))$. Then

$$C_{i,j} = \sum \prod_{\beta \in \mathbb{F}_q} \binom{n_i(\beta)}{\nu_\beta}, \quad (51)$$

where the sum runs over all the sets of integers $\{\nu_\beta\}_{\beta \in \mathbb{F}_q}$ ($0 \leq \nu_\beta \leq n_i(\beta)$), satisfying

$$\sum_{\beta \in \mathbb{F}_q} \nu_\beta = j \text{ and } \sum_{\beta \in \mathbb{F}_q} \nu_\beta \beta = 0. \quad (52)$$

Corollary 17 : Let $\{C_{i,j}\}_{j=0}^{N_i}$ be the weight distribution of $C(G_i(q))$, for $i = 1, 2, 3$. Then, for $i = 1, 2, 3$, we have: $C_{i,j} = C_{i,N_i-j}$, for all j , with $0 \leq j \leq N_i$.

PROOF. Under the replacements $\nu_\beta \rightarrow n_i(\beta) - \nu_\beta$, for each $\beta \in \mathbb{F}_q$, the first equation in (52) is changed to $N_i - j$, while the second one in (52) and the summands in (51) are left unchanged. Here the second sum in (52) is left unchanged, since $\sum_{\beta \in \mathbb{F}_q} n_i(\beta) \beta = 0$, as one can see by using the explicit expression of $n_i(\beta)$ in (40)-(42). \square

Theorem 18 ([12]): Let $q = 2^r$, with $r \geq 2$. Then the range R of $K(\lambda; a)$, as a varies over \mathbb{F}_q^* , is given by:

$$R = \{t \in \mathbb{Z} \mid |t| < 2\sqrt{q}, t \equiv -1 \pmod{4}\}.$$

In addition, each value $t \in R$ is attained exactly $H(t^2 - q)$ times, where $H(d)$ is the Kronecker class number of d .

Now, we get the following formulas in (2), (5), and (8), by applying the formula in (51) to each $C(G_i(q))$, using the explicit values of $n_i(\beta)$ in (40)-(42), and taking Theorem 18 into consideration.

Theorem 19 : Let $\{C_{i,j}\}_{j=0}^{N_i}$ be the weight distribution of $C(G_i(q))$, for $i = 1, 2, 3$. Then

$$(a) \quad C_{1,j} = \sum \binom{1}{\nu_0} \prod_{\text{tr}(\beta^{-1})=1} \binom{2}{\nu_\beta} \quad (j = 0, \dots, N_1),$$

where the sum is over all the sets of nonnegative integers $\{\nu_0\} \cup \{\nu_\beta\}_{\text{tr}(\beta^{-1})=1}$ satisfying $\nu_0 + \sum_{\text{tr}(\beta^{-1})=1} \nu_\beta = j$ and $\sum_{\text{tr}(\beta^{-1})=1} \nu_\beta \beta = 0$.

$$(b) \quad C_{2,j} = \sum \binom{q+2}{\nu_0} \prod_{\text{tr}(\beta^{-1})=1} \binom{2}{\nu_\beta} \quad (j = 0, \dots, N_2),$$

where the sum is over all the sets of nonnegative integers $\{\nu_0\} \cup \{\nu_\beta\}_{\text{tr}(\beta^{-1})=1}$ satisfying $\nu_0 + \sum_{\text{tr}(\beta^{-1})=1} \nu_\beta = j$ and $\sum_{\text{tr}(\beta^{-1})=1} \nu_\beta \beta = 0$.

$$(c) \quad C_{3,j} = \sum \binom{m_0}{\nu_0} \prod_{|t| < 2\sqrt{q}, t \equiv -1(4)} \prod_{K(\lambda; \beta^{-1})=t} \binom{m_t}{\nu_\beta} \quad (j = 0, \dots, N_3),$$

where the sum is over all the sets of nonnegative integers $\{\nu_\beta\}_{\beta \in \mathbb{F}_q}$ satisfying $\sum_{\beta \in \mathbb{F}_q} \nu_\beta = j$ and $\sum_{\beta \in \mathbb{F}_q} \nu_\beta \beta = 0$,

$$m_0 = q^4,$$

and

$$m_t = q^2(q^3 + q^2 - t),$$

for all integers t satisfying $|t| < 2\sqrt{q}$ and $t \equiv -1(\text{mod } 4)$.

We now apply the Pless power moment identity in (48) to each $C(G_i(q))^\perp$, for $i = 1, 2, 3$, in order to obtain the results in Theorem 1(cf. (1), (4), (6), (7)) about recursive formulas.

Then the left hand side of that identity in (48) is equal to

$$\sum_{a \in \mathbb{F}_q^*} w(c(a))^h, \tag{53}$$

with the $w(c(a))$ in each case given by (49), (50).

For $i = 1, 2$, (53) is

$$\begin{aligned}
& \frac{1}{2^h} \sum_{a \in \mathbb{F}_q^*} (q + 1 + K(\lambda; a))^h \\
&= \frac{1}{2^h} \sum_{a \in \mathbb{F}_q^*} \sum_{l=0}^h \binom{h}{l} (q + 1)^{h-l} K(\lambda; a)^l \\
&= \frac{1}{2^h} \sum_{l=0}^h \binom{h}{l} (q + 1)^{h-l} M K^l.
\end{aligned} \tag{54}$$

Similarly, for $i = 3$, (53) equals

$$\left(\frac{q^2}{2}\right)^h \sum_{l=0}^h \binom{h}{l} (q^4 + q^3 - q - 1)^{h-l} M K^{2l} \tag{55}$$

$$= \left(\frac{q^2}{2}\right)^h \sum_{l=0}^h \binom{h}{l} (q^4 + q^3 - 1)^{h-l} M K_2^l. \tag{56}$$

Note here that, in view of (32), obtaining power moments of 2-dimensional Kloosterman sums is equivalent to getting even power moments of Kloosterman sums. Also, one has to separate the term corresponding to $l = h$ in (54)-(56), and notes $\dim_{\mathbb{F}_2} C(G_i) = r$.

6 Remarks and Examples

The explicit computations about power moments of Kloosterman sums was begun with the paper [18] of Salié in 1931, where he showed, for any odd prime q ,

$$M K^h = q^2 M_{h-1} - (q - 1)^{h-1} + 2(-1)^{h-1} \quad (h \geq 1). \tag{57}$$

However, this holds for any prime power $q = p^r$ (p a prime). Here $M_0 = 0$, and for $h \in \mathbb{Z}_{>0}$,

$$M_h = |\{(\alpha_1, \dots, \alpha_h) \in (\mathbb{F}_q^*)^h \mid \sum_{j=1}^h \alpha_j = 1 = \sum_{j=1}^h \alpha_j^{-1}\}|.$$

For positive integers h , we let

$$A_h = |\{(\alpha_1, \dots, \alpha_h) \in (\mathbb{F}_q^*)^h \mid \sum_{j=1}^h \alpha_j = 0 = \sum_{j=1}^h \alpha_j^{-1}\}|.$$

Then $(q-1)M_{h-1} = A_h$, for any $h \in \mathbb{Z}_{>0}$. So (57) can be rewritten as

$$MK^h = \frac{q^2}{q-1}A_h - (q-1)^{h-1} + 2(-1)^{h-1}. \quad (58)$$

Iwaniec [5] showed the expression (58) for any prime q . However, the proof given there works for any prime power q , without any restriction. Also, this is a special case of Theorem 1 in [3], as mentioned in Remark 2 there.

For $q = p$ any prime, MK^h was determined for $h \leq 4$ (cf. [5], [18]).

$$MK^1 = 1, \quad MK^2 = p^2 - p - 1,$$

$$MK^3 = \left(\frac{-3}{p}\right)p^2 + 2p + 1 \text{ (with the understanding } \left(\frac{-3}{2}\right) = -1 \text{ (}\frac{-3}{3}\right) = 0),$$

$$MK^4 = \begin{cases} 2p^3 - 3p^2 - 3p - 1, & p \leq 3, \\ 1, & p = 2. \end{cases}$$

Except [1] for $1 \leq h \leq 4$, not much progress had been made until Moisiu succeeded in evaluating MK^h , for the other values of h with $h \leq 10$ over the finite fields of characteristic two in [15] (Similar results exist also over the finite fields of characteristic three (cf. [4], [16])). So we have now closed form formulas for $h \leq 10$.

His result was a breakthrough, but the way it was proved is too indirect, since the frequencies are expressed in terms of the Eichler Selberg trace formulas for the Hecke operators acting on certain spaces of cusp forms for $\Gamma_1(4)$. In addition, the power moments of Kloosterman sums are obtained only for $h \leq 10$ and not for any higher order moments. On the other hand, our formulas in (1) and (2) allow one, at least in principle, to compute moments of all orders for any given q .

In below, for small values of i , we compute, by using (1), (2), and MAGMA, the frequencies C_i of weights in $C(SO^-(2, 2^4))$ and $C(SO^-(2, 2^5))$, and the power moments MK^h of Kloosterman sums over \mathbb{F}_{2^4} and \mathbb{F}_{2^5} . In particular, our results confirm those of Moisiu's given in [15], when $q = 2^4$ and $q = 2^5$.

TABLE I
The weight distribution of $C(SO^-(2, 2^4))$

w	frequency	w	frequency	w	frequency	w	frequency
0	1	5	396	10	1208	15	8
1	1	6	792	11	792	16	1
2	8	7	1208	12	396	17	1
3	40	8	1510	13	140		
4	140	9	1510	14	40		

TABLE II
The power moments of Kloosterman sums over \mathbb{F}_{2^4}

i	MK^i	i	MK^i	i	MK^i
0	15	10	604249199	20	159966016268924111
1	1	11	3760049569	21	1115184421375168321
2	239	12	28661262671	22	7829178965854277039
3	289	13	188901585601	23	54689811340914235489
4	7631	14	1380879340079	24	383400882469952537231
5	22081	15	9373110103009	25	2680945149821576426881
6	300719	16	67076384888591	26	18780921149940510987119
7	1343329	17	462209786722561	27	131394922435183254906529
8	13118351	18	3272087534565359	28	920122084792925568335951
9	72973441	19	22721501074479649	29	6439066453841188580322241

TABLE III
The weight distribution of $C(SO^-(2, 2^5))$

w	frequency	w	frequency	w	frequency	w	frequency
0	1	9	1204220	18	32411632	27	34800
1	1	10	2892592	19	25586000	28	7352
2	16	11	6049808	20	17909672	29	1240
3	176	12	11088968	21	11088968	30	176
4	1240	13	17909672	22	6049808	31	16
5	7352	14	25586000	23	2892592	32	1
6	34800	15	32411632	24	1204220	33	1
7	133840	16	36463878	25	433532		
8	433532	17	36463878	26	133840		

TABLE IV
The power moments of Kloosterman sums over \mathbb{F}_{25}

i	MK^i	i	MK^i	i	MK^i
0	31	10	44833141471	20	733937760431358760351
1	1	11	138050637121	21	6855945343839827241601
2	991	12	4621008512671	22	86346164924243497892191
3	-959	13	22291740481921	23	851252336789971927746241
4	63391	14	497555476630111	24	10249523095374924648418591
5	-63359	15	3171377872090561	25	104764273348415132423811841
6	5102431	16	55381758830599711	26	1224170008071148563308433631
7	-678719	17	423220459165032961	27	12819574031043721011365916481
8	460435231	18	6318551635327312351	28	146828974390583504114568758431
9	613044481	19	54461730980167425601	29	1562774752282717527826758007681

References

- [1] L. Carlitz, “Gauss sums over finite fields of order 2^n ,” Acta Arith. vol. 15, pp. 247-265, 1969.
- [2] L. Carlitz, “A note on exponential sums,” Pacific J. Math., vol. 30, pp. 35-37, 1969.
- [3] Hi-joon Chae and D. S. Kim, “A generalization of power moments of Kloosterman sums,” Arch. Math.(Basel), vol. 89, pp. 152-156, 2007.
- [4] G. van der Geer, R. Schoof and M. van der Vlugt, “Weight formulas for ternary Melas codes,” Math. Comp., vol. 58, pp. 781-792, 1992.
- [5] H. Iwaniec, Topics in Classical Automorphic Forms, Amer. Math. Soc., Providence, R. I., 1997.
- [6] D. S. Kim, “Gauss sums for symplectic groups over a finite field,” Mh. Math., vol.126, pp. 55-71, 1998.
- [7] D. S. Kim, “Codes associated with special linear groups and power moments of multi-dimensional Kloosterman sums,” preprint(2008), arXiv:0807.3991v1 [math.NT].
- [8] D. S. Kim, “Codes associated with $O^+(2n, 2^r)$ and power moments of Kloosterman sums,” preprint(2008), arXiv:0807.4671v1 [math.NT].
- [9] D. S. Kim, “Exponential sums for $O^-(2n, q)$ and their applications,” Acta Arith., vol. 82, pp. 331-357, 1997.
- [10] D. S. Kim and Y. H. Park, “Gauss sums for orthogonal groups over a finite field of characteristic two,” Acta Arith., vol. 97, pp. 67-86, 2001.
- [11] H. D. Kloosterman, “On the representation of numbers in the form $ax^2 + by^2 + cz^2 + dt^2$,” Acta Math. vol. 49, pp. 407-464, 1926.
- [12] G. Lachaud and J. Wolfmann, “The weights of the orthogonals of the extended quadratic binary Goppa codes,” IEEE Trans. Inform. Theory, vol. 36, pp. 686-692, 1990.
- [13] R. Lidl and H. Niederreiter, Finite Fields, 2nd ed. Cambridge, U. K.: Cambridge University Press, 1997, vol.20, Encyclopedia of Mathematics and Its Applications.
- [14] F. J. MacWilliams and N. J. A. Sloane, The Theory of Error Correcting Codes, Amsterdam, The Netherlands: North-Holland, 1998.
- [15] M. Moisio, “The moments of a Kloosterman sum and the weight distribution of a Zetterberg-type binary cyclic code,” IEEE Trans. Inform. Theory, vol. 53, pp. 843-847, 2007.
- [16] M. Moisio, “On the moments of Kloosterman sums and fibre products of Kloosterman curves,” Finite Fields Appl., vol.14, pp. 515-531, 2008.

- [17] M.Moisio, “Kloosterman sums, elliptic curves, and irreducible polynomials with prescribed trace and norm,” *Acta Arith.*, to appear.
- [18] H. Salié, “Über die Kloostermanschen Summen $S(u, v; q)$,” *Math. Z.*, vol. 34, pp. 91-109, 1931.
- [19] R. Schoof and M. van der Vlugt, “Hecke operators and the weight distributions of certain codes,” *J. Combin. Theory Ser. A*, vol. 57, pp.163-186, 1991.
- [20] Z.-X. Wan, “Geometry of Classical Groups over Finite Fields,” *Studentlitteratur*, Lund, 1993.